La Revue de la BNU

13 | 2016
Varia 13

De la dissimulation du sens à la protection des données : petite histoire de la cryptologie

Valérie Caniart

Édition électronique
URL : http://journals.openedition.org/rbnu/1482
DOI : 10.4000/rbnu.1482
ISSN : 2679-6104

Éditeur
Bibliothèque nationale et universitaire de Strasbourg

Édition imprimée
Date de publication : 1 mai 2016
Pagination : 24-35
ISBN : 9782859230623
ISSN : 2109-2761

Référence électronique
Valérie Caniart, « De la dissimulation du sens à la protection des données : petite histoire de la cryptologie », *La Revue de la BNU* [En ligne], 13 | 2016, mis en ligne le 01 mars 2020, consulté le 12 décembre 2020. URL : http://journals.openedition.org/rbnu/1482 ; DOI : https://doi.org/10.4000/rbnu.1482

TRAICTÉ

DES CHIFFRES,

OV SECRETES MANIERES D'ESCRIRE:

PAR

BLAISE DE VIGENERE,

BOVRBONNOIS.

A PARIS,

Chez ABEL L'ANGELIER, au premier pillier de la grand' Salle du Palais.

M. D. LXXXVI.

AVEC PRIVILEGE DV ROY.

Page de titre du *Traicté des chiffres, ou secrètes manières d'escrire* de Blaise de Vigenère (Paris, L'Angelier, 1586 ; coll. BNU)

DE LA DISSIMULATION DU SENS À LA PROTECTION DES DONNÉES : petite histoire de la cryptologie

La cryptographie, ou l'art de dissimuler le sens d'un texte à l'attention d'une tierce personne, est une pratique presque aussi ancienne que l'écriture elle-même. Il semblerait que le texte au sens dissimulé le plus ancien qui ait été retrouvé soit de nature économique : il s'agit d'une tablette mésopotamienne datant d'environ 1500 av. J.-C. et recelant la formule d'un vernis à poteries. Ainsi, dès la plus haute Antiquité, l'homme a tenté de dissimuler des informations de toute nature : politique, militaire, économique. C'est toutefois dans les sphères politiques que ce stratagème a été le plus utilisé, à partir du 16e siècle, date à laquelle les fondements de cette science ont été posés.

Aujourd'hui, cet usage est extrêmement répandu. La cryptographie n'est plus réservée aux seules sphères du pouvoir et de la diplomatie, mais elle est utilisée quotidiennement par tous ceux qui ont des informations à protéger, les entreprises comme les particuliers. Ainsi, à l'ère d'Internet et des objets connectés, les transactions des utilisateurs de la Toile sont protégées par des procédés cryptographiques avancés. Les techniques de camouflages se sont tellement complexifiées qu'elles sont devenues un domaine des mathématiques à part entière. Enfin, depuis le 20e siècle, on ne parle plus de cryptographie mais de cryptologie.

Cette science nouvelle à l'histoire très ancienne est encore méconnue. L'historiographie est très récente puisqu'elle commence avec l'ouvrage, encore inégalé, de l'historien américain David Kahn, *Code Breakers, the Story of Secret Writings*, paru en 1967. Le sujet est relativement difficile à traiter et il suffit de parcourir les nombreux ouvrages pour s'en apercevoir. Se limiter à un aperçu historique fait prendre le risque d'énumérer de nombreuses anecdotes, la plupart relativement bien connues, mettant en scène le rôle joué par des messages décryptés qui ont changé le cours de l'Histoire, ou du moins l'issue d'une bataille, ou encore favorisé un retournement de situation, dans le but avoué de montrer l'importance de cette pratique de l'ombre. L'autre travers serait de tomber dans un discours purement technique, décrivant les différents procédés de chiffrement. Il en résulterait un discours austère et indigeste, décourageant très vite le non-initié.

À travers les trois grandes périodes reconnues par les spécialistes, que Jacques Stern a qualifiées de période artisanale, période mécanique et ère moderne[1], et tout en reprenant la mise en garde de David Kahn, de « [...] veiller à ne pas attribuer à la seule cryptographie tout le mérite d'une victoire ou d'un succès diplomatique », l'objectif de cet article est de montrer que l'évolution des techniques de chiffrement accompagne en fait celle de toute société qui s'épanouit sur les échanges et le partage de l'information.

L'ère artisanale ou la cryptographie manuelle

La première période, très longue, s'étend sur plusieurs siècles, de l'Antiquité à la veille de la Première Guerre mondiale. Il s'agit en fait d'une longue maturation et de mises au point de procédés et principes qui se sont développés de façon très sporadique. On peut parler de cryptographie manuelle, parce que la seule ressource est l'ingéniosité et la puissance de calcul des hommes chargés de développer et d'appliquer les méthodes de

chiffrement. Cette période peut elle-même être découpée en trois temps : l'Antiquité, un premier sursaut aux 16e-17e siècles, puis l'essor définitif dans la seconde partie du 19e siècle.

De l'Antiquité, trois procédés sont parvenus jusqu'à nous à travers quelques écrits attestant de leur existence et de leur emploi : la scytale des Lacédémoniens, le carré de Polybe et l'alphabet de Jules César.

La première est décrite par l'historien Thucydide comme ayant été inventée à Sparte au 4e siècle avant notre ère. Il s'agit d'un bâton cylindrique en bois d'un diamètre déterminé, dont la surface est taillée de façon à former plusieurs facettes. Une longue bandelette de cuir, tissu ou papyrus est ensuite enroulée autour. Le message est inscrit en suivant les facettes du cylindre. La bandelette déroulée ne laisse donc plus apparaître qu'une suite de lettres sans signification. L'historien Polybe, quant à lui, invente au 2e siècle av. J.-C. un procédé de chiffrement connu sous le nom de carré de Polybe ou carré de 25. Il s'agit d'une grille de 25 cases (mais on peut aller jusqu'à 36 pour y faire figurer des chiffres), dont on numérote la première ligne et la première colonne. Le reste est rempli des lettres de l'alphabet. Le principe est de remplacer chaque lettre par ses coordonnées dans le tableau. Enfin, les écrits de Jules César laissent entendre que celui-ci utilisait comme moyen de chiffrement un alphabet décalé, appelé depuis alphabet de César. Mais en dehors de ces traces épistémologiques attestant de pratiques de chiffrement de textes, il ne reste aucun témoignage de théorisation sur le chiffre.

Après la chute de l'empire romain d'Occident et pendant tout le haut Moyen Âge, les historiens s'accordent pour dire que ces procédés tombent dans l'oubli. L'une des raisons est probablement le recul de l'écrit. À l'image de Charlemagne, dont la légende dit qu'il ne savait pas lire, la plupart des seigneurs formant l'élite guerrière sont illettrés ; la lecture et l'écriture sont l'apanage des seuls ecclésiastiques. L'écriture constitue par elle-même un moyen de chiffrement, tandis que l'Église condamne tout usage de chiffre. Les connaissances héritées de l'Antiquité sont perpétuées dans le monde arabe. Le plus ancien texte connu décrivant une méthode de décryptement est rédigé au 9e siècle par le philosophe al-Kindi [2], connu également sous le nom latinisé d'Achindius.

C'est sans doute par ce biais qu'est redécouverte cette technique en Occident au 15e siècle, d'abord en Italie, dans les États du pape, la République de Venise et dans les puissantes cités de Milan ou Mantoue, puis en France et dans une moindre mesure en Allemagne et en Angleterre. Il est intéressant de noter l'apparition au 15e siècle du terme « chiffre », issu de l'arabe « sifr ». Il désigne l'ensemble des conventions qui permettent de transformer un texte « clair », c'est-à-dire intelligible par tous, en texte « chiffré » donc illisible par qui ne possède pas la convention, et inversement. Par extension, le mot « chiffreur » fait son apparition dès le premier quart du 16e siècle pour désigner celui qui transcrit un texte en clair ou en chiffré. Du 16e au 17e siècle, l'emploi de chiffres s'impose dans les relations diplomatiques et au plus haut niveau du commandement militaire. Ce développement aboutit à l'apparition du mot « cryptographie », au début du 17e siècle, mot qui signifie alors « science du chiffre » ou « art des écritures secrètes », indiquant par là-même une certaine codification et normalisation des pratiques.

Ainsi, Alberti rédige ce qui peut être considéré comme le premier traité de cryptographie où est décrit un procédé de chiffrement par substitution, invente un cryptographe, le Cadran d'Alberti, et s'intéresse au déchiffrement en réalisant la première analyse linguistique sur la fréquence des lettres et des digrammes dans les langues latine et italienne. En Italie toujours, Jérôme Cardan (Gerolamo Cardano, 1501-1576) invente quant à lui la fameuse grille de Cardan, décrite ainsi par Edmond Lerville : « Cette grille comporte un certain nombre de fentes égal au quart des cases, disposées de telle manière que des rotations successives de 90° découvrent successivement toutes les cases de la grille. Le message à transmettre est écrit successivement dans chaque portion de la grille. On obtient donc une transposition » [3]. Ces réflexions sont divulguées grâce aux livres et l'intérêt déborde largement des frontières.

En France, Blaise de Vigenère, après avoir étudié le chiffre à Rome lors d'un voyage en 1549, fait paraître un *Traicté des chiffres, ou secrètes manières d'escrire* en 1586, dans lequel il décrit un système de chiffrement par substitution à double clé qu'il appelle le système indéchiffrable. Il le resta en effet assez longtemps. Le déchiffrement est quant à lui étudié par François Viète (1540-1630), attaché au service d'Henri IV.

Enfin, il faut nommer Antoine Rossignol (1590-1673), féru de cryptographie et propriétaire d'une bibliothèque rassemblant tous les ouvrages de l'époque sur le sujet, appelé au service du Roi pour déchiffrer des dépêches huguenotes et anglaises. À la vue des résultats hautement satisfaisants (capitulation de la ville de Réalmont dans le Tarn en 1627 et de La Rochelle en 1628), Richelieu l'attacha définitivement à son service et lui demanda de créer

OUVRAGES DU MÊME AUTEUR :

L'Art monumental dans ses rapports avec les idées religieuses. Paris, Claye, in-8°.

Daniel Casper von Lohenstein's Trauerspiele, mit besonderer Berücksichtigung der Kleopatra. Paderborn, Schœningh, in-8°.

Letterkundige Studien over de Vlaamsche Taal. Malines, Olbrechts, in-8°.

Grammaire anglaise, à l'usage des classes élémentaires. Paris, Hachette et C^ie^, in-12.

Nouvelle Méthode pour apprendre facilement les Déclinaisons allemandes. Paris, Hachette et C^ie^, in-12.

Paris. — Imprimerie L. Baudoin et C^ie^, rue Christine, 2

LA

CRYPTOGRAPHIE MILITAIRE

OU

DES CHIFFRES USITÉS EN TEMPS DE GUERRE

AVEC UN

Nouveau procédé de déchiffrement applicable aux systèmes à double clef

PAR

Aug. KERCKHOFFS

Docteur ès lettres
Professeur à l'École des Hautes Études commerciales et à l'École Arago
Membre de la Société française d'Archéologie
et de Numismatique, de la Société d'Archéologie de Seine-et-Marne, etc.
Commandeur de l'Ordre militaire du Christ,
Officier d'académie.

La cryptographie est un auxiliaire puissant de la tactique militaire.
(Général Lewal, *Études de guerre.*)

PARIS
LIBRAIRIE MILITAIRE DE L. BAUDOIN ET C^ie^
LIBRAIRES-ÉDITEURS
SUCCESSEURS DE J. DUMAINE
30, Rue et Passage Dauphine, 30

1883

Première page du tiré-à-part de l'ouvrage d'Auguste Kerckhoffs. Celui-ci peut être considéré comme le premier ouvrage théorique du chiffre militaire en langue française (coll. Musée des transmissions).

le premier service du chiffre en France[4]. Rossignol est l'auteur du Grand Chiffre de Louis XIV, resté indéchiffré jusqu'au début du 20e siècle. Sa légendaire efficacité dans le déchiffrement lui valut de donner son nom à ce petit instrument destiné à crocheter les serrures.

À travers leurs écrits, ces différents auteurs décrivent les principes de chiffrement sur lesquels repose toute méthode[5] : le principe de transposition, ou mélange des lettres du message, et celui de la substitution ou remplacement des lettres par d'autres signes. Ils s'intéressent tout autant au chiffrement qu'à la cryptanalyse, c'est-à-dire au moyen de casser un chiffre.

Le contexte dans lequel se développe la cryptographie est tout aussi important. L'invention de l'imprimerie autour de 1453 révolutionne le monde occidental et accompagne le mouvement intellectuel de la Renaissance. Elle permet à une plus grande frange de la société d'accéder à l'écrit et de découvrir les textes des auteurs antiques, jusque-là réservés aux savants des monastères. Par conséquent, ce seul développement de l'écrit pourrait amener à penser qu'il devient nécessaire de dissimuler des informations susceptibles d'être interceptées par un plus grand nombre de personnes. Mais il est permis de penser que ce n'est pas une raison suffisante. Cette période de florissement intellectuel est également celle d'une expansion économique sans précédent, due à de multiples améliorations (techniques agricoles permettant une meilleure productivité, techniques de navigation favorisant l'expansion coloniale et commerciale, apparition de nouvelles structures financières, etc.) et dont l'aboutissement est l'émergence d'une nouvelle classe sociale, la bourgeoisie. Il existe donc un plus grand nombre de personnes détenant des informations ou des intérêts suffisamment importants pour vouloir les dissimuler à d'éventuels concurrents.

À partir de la seconde moitié du 17e siècle, le chiffre entre dans une période de déclin, suscitant peu d'études, ne révélant aucun auteur digne d'intérêt, tandis que la mise en œuvre des procédés de chiffrement tombe au plus bas, jusqu'à la première moitié du 19e siècle. S'ouvre alors la troisième et dernière période de cet âge artisanal, le dernier quart du 19e siècle.

Deux raisons principales favorisent le renouveau de la cryptographie, en particulier en France : l'invention et le développement du télégraphe et la réforme en profondeur de l'armée française après la défaite humiliante de 1870.

La pose du premier câble transatlantique en 1866 marque un tournant dans l'usage du télégraphe électrique. La circulation de messages de toutes natures, commerciales, financières, politiques, dont certains sont susceptibles de comporter des informations capitales, sur les lignes télégraphiques étrangères les mettent à la merci de toutes les indiscrétions. Cela fait réfléchir à la nécessité de protéger les informations. Mais plus encore, ce sont les tarifs d'expédition pratiqués par les compagnies télégraphiques exploitantes qui incitent à revoir les procédés de chiffrement. Une anecdote permet de prendre la mesure de cette contrainte économique.

> Le Grand Chiffre de Louis XIV est resté indéchiffré jusqu'au début du 20e siècle.

En 1867, peu après l'établissement sur le trône du Mexique de Maximilien d'Autriche par des troupes françaises envoyées sur place, le secrétaire d'État américain William Seward expédie à Paris une dépêche demandant le retrait des troupes françaises. Le télégramme, chiffré au moyen du code diplomatique alors en usage dans les ambassades américaines, comporte 1 100 groupes de 3, 4 ou 5 chiffres. Les télégrammes étant alors facturés à la lettre, le montant s'élève à 23 000 $[6] ! Seward, refusant de payer une telle somme, entame des négociations pour obtenir des tarifs plus favorables à son administration. En France, le bureau du chiffre du ministère des Affaires étrangères est confronté au même problème et se donne pour objectif de baisser de 40 % les frais d'expédition des télégrammes chiffrés[7].

Du côté militaire, la guerre de 1870 a révélé deux défaillances dans le domaine des transmissions : l'inadaptation du service télégraphique et le manque de moyens de chiffrement qui dépendaient alors uniquement des Affaires étrangères. C'est donc avec des préoccupations d'emploi que les premiers théoriciens commencent à réfléchir au chiffre. Dans une étude critique sur l'armée et les réformes à y introduire, le général Lewal[8] définit pour la première fois en 1881 le chiffre militaire et les besoins de

Archives N° 1

MINISTÈRE DE LA GUERRE

SECRET

ÉTAT-MAJOR DE L'ARMÉE

CODE DE SERVICE T. S. F.

2e PARTIE

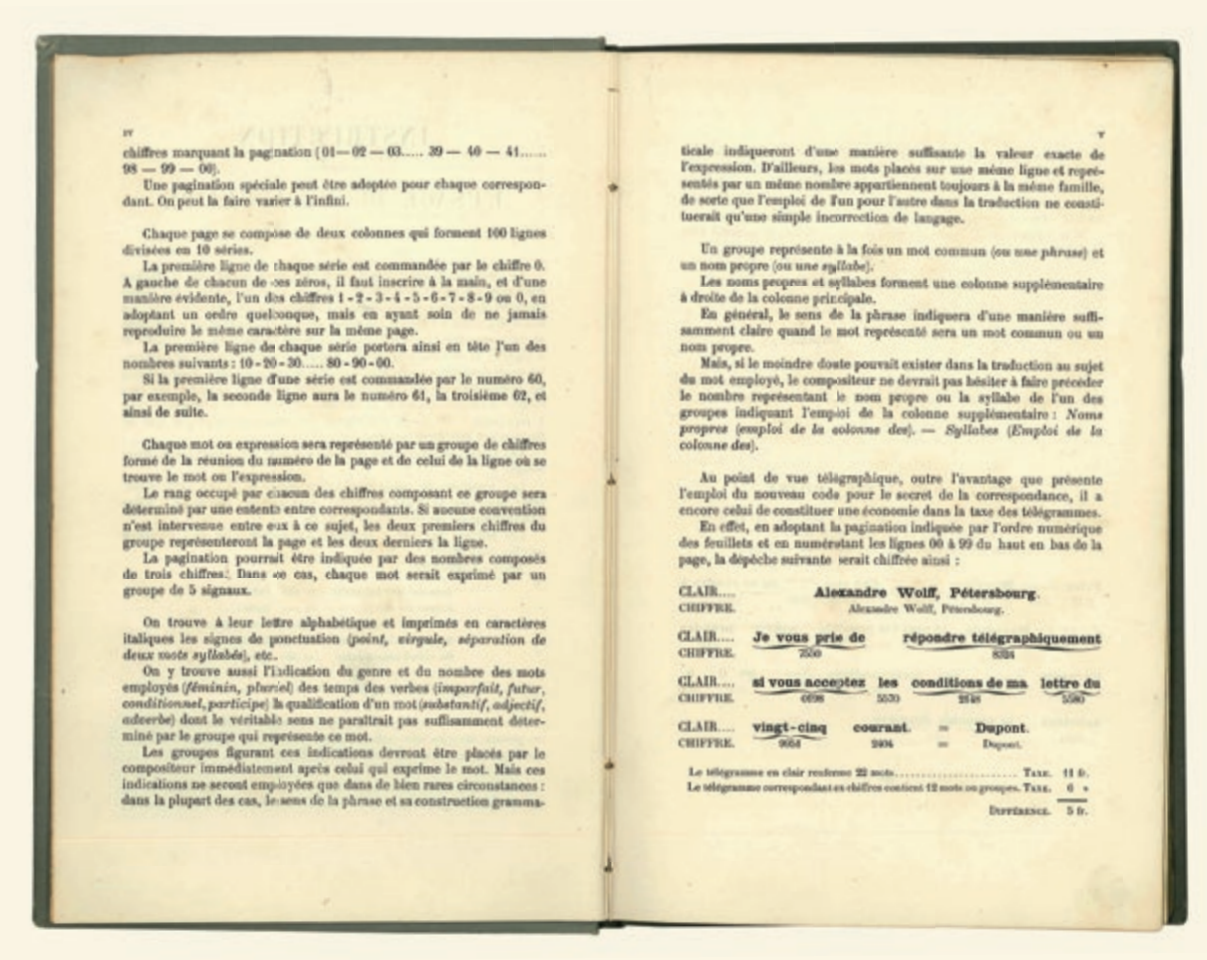
CARNET DE CHIFFRE SPÉCIAL T. S. F.

PARIS

IMPRIMERIE NATIONALE

1929

Page de couverture du code de service TSF en usage au ministère de la Guerre pour les transmissions d'ordre technique ou les radiotélégrammes de services (coll. Musée des transmissions).



IV

chiffres marquant la pagination (01 — 02 — 03..... 39 — 40 — 41..... 98 — 99 — 00).

Une pagination spéciale peut être adoptée pour chaque correspondant. On peut la faire varier à l'infini.

Chaque page se compose de deux colonnes qui forment 100 lignes divisées en 10 séries.

La première ligne de chaque série est commandée par le chiffre 0. A gauche de chacun de ces zéros, il faut inscrire à la main, et d'une manière évidente, l'un des chiffres 1 - 2 - 3 - 4 - 5 - 6 - 7 - 8 - 9 ou 0, en adoptant un ordre quelconque, mais en ayant soin de ne jamais reproduire le même caractère sur la même page.

La première ligne de chaque série portera ainsi en tête l'un des nombres suivants : 10 - 20 - 30..... 80 - 90 - 00.

Si la première ligne d'une série est commandée par le numéro 60, par exemple, la seconde ligne aura le numéro 61, la troisième 62, et ainsi de suite.

Chaque mot ou expression sera représenté par un groupe de chiffres formé de la réunion du numéro de la page et de celui de la ligne où se trouve le mot ou l'expression.

Le rang occupé par chacun des chiffres composant ce groupe sera déterminé par une entente entre correspondants. Si aucune convention n'est intervenue entre eux à ce sujet, les deux premiers chiffres du groupe représenteront la page et les deux derniers la ligne.

La pagination pourrait être indiquée par des nombres composés de trois chiffres. Dans ce cas, chaque mot serait exprimé par un groupe de 5 signaux.

On trouve à leur lettre alphabétique et imprimés en caractères italiques les signes de ponctuation (*point, virgule, séparation de deux mots syllabés*), etc..

On y trouve aussi l'indication du genre et du nombre des mots employés (*féminin, pluriel*) des temps des verbes (*imparfait, futur, conditionnel, participe*) la qualification d'un mot (*substantif, adjectif, adverbe*) dont le véritable sens ne paraîtrait pas suffisamment déterminé par le groupe qui représente ce mot.

Les groupes figurant ces indications devront être placés par le compositeur immédiatement après celui qui exprime le mot. Mais ces indications ne seront employées que dans de bien rares circonstances : dans la plupart des cas, le sens de la phrase et sa construction grammaticale indiqueront d'une manière suffisante la valeur exacte de l'expression. D'ailleurs, les mots placés sur une même ligne et représentés par un même nombre appartiennent toujours à la même famille, de sorte que l'emploi de l'un pour l'autre dans la traduction ne constituerait qu'une simple incorrection de langage.

V

Un groupe représente à la fois un mot commun (ou une *phrase*) et un nom propre (ou une *syllabe*).

Les noms propres et syllabes forment une colonne supplémentaire à droite de la colonne principale.

En général, le sens de la phrase indiquera d'une manière suffisamment claire quand le mot représenté sera un mot commun ou un nom propre.

Mais, si le moindre doute pouvait exister dans la traduction au sujet du mot employé, le compositeur ne devrait pas hésiter à faire précéder le nombre représentant le nom propre ou la syllabe de l'un des groupes indiquant l'emploi de la colonne supplémentaire : *Noms propres (emploi de la colonne des)*. — *Syllabes (Emploi de la colonne des)*.

Au point de vue télégraphique, outre l'avantage que présente l'emploi du nouveau code pour le secret de la correspondance, il a encore celui de constituer une économie dans la taxe des télégrammes.

En effet, en adoptant la pagination indiquée par l'ordre numérique des feuillets et en numérotant les lignes 00 à 99 du haut en bas de la page, la dépêche suivante serait chiffrée ainsi :

CLAIR.... **Alexandre Wolff, Pétersbourg.**
CHIFFRE. Alexandre Wolff, Pétersbourg.

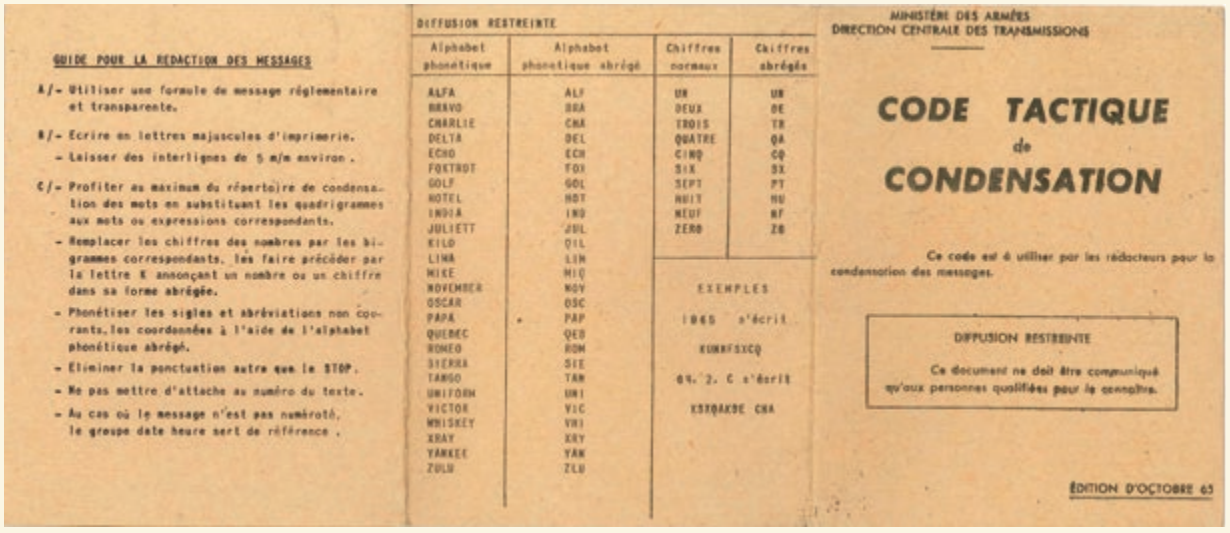
CLAIR.... **Je vous prie de** **répondre télégraphiquement**
CHIFFRE. 2500 8504

CLAIR.... **si vous acceptez** **les** **conditions de ma** **lettre du**
CHIFFRE. 6098 5020 2148 5580

CLAIR.... **vingt-cinq** **courant.** = **Dupont.**
CHIFFRE. 9054 2404 = Dupont.

Le télégramme en clair renferme 22 mots..... TAXE. 11 f.
Le télégramme correspondant en chiffres contient 12 mots en groupes. TAXE. 6 »
DIFFÉRENCE. 5 f.

Extrait de l'instruction pour l'usage du vocabulaire administratif et commercial
(in *Nouveau code ou vocabulaire administratif et commercial pour la correspondance secrète*,
par Nilac, Paris, Librairie étrangère, 1891 ; coll. Musée des transmissions).



GUIDE POUR LA REDACTION DES MESSAGES

A/- Utiliser une formule de message réglementaire et transparente.

B/- Ecrire en lettres majuscules d'imprimerie.
- Laisser des interlignes de 5 m/m environ.

C/- Profiter au maximum du répertoire de condensation des mots en substituant les quadrigrammes aux mots ou expressions correspondants.
- Remplacer les chiffres des nombres par les bigrammes correspondants, les faire précéder par la lettre K annonçant un nombre ou un chiffre dans sa forme abrégée.
- Phonétiser les sigles et abréviations non courants, les coordonnées à l'aide de l'alphabet phonétique abrégé.
- Eliminer la ponctuation autre que le STOP.
- Ne pas mettre d'attache au numéro du texte.
- Au cas où le message n'est pas numéroté, le groupe date heure sert de référence.

DIFFUSION RESTREINTE

Alphabet phonétique	Alphabet phonétique abrégé	Chiffres normaux	Chiffres abrégés
ALFA	ALF	UN	UN
BRAVO	BRA	DEUX	DE
CHARLIE	CHA	TROIS	TR
DELTA	DEL	QUATRE	QA
ECHO	ECH	CINQ	CQ
FOXTROT	FOX	SIX	SX
GOLF	GOL	SEPT	PT
HOTEL	HOT	HUIT	HU
INDIA	IND	NEUF	NF
JULIETT	JUL	ZERO	ZR
KILO	QIL		
LIMA	LIM		
MIKE	MIQ		
NOVEMBER	NOV		
OSCAR	OSC		
PAPA	PAP		
QUEBEC	QEB		
ROMEO	ROM		
SIERRA	SIE		
TANGO	TAN		
UNIFORM	UNI		
VICTOR	VIC		
WHISKEY	WHI		
XRAY	XRY		
YANKEE	YAN		
ZULU	ZLU		

EXEMPLES

1965 s'écrit
KUNFSXCQ

69, 2, C s'écrit
KSIXAXDE CNA

MINISTÈRE DES ARMÉES
DIRECTION CENTRALE DES TRANSMISSIONS

CODE TACTIQUE de CONDENSATION

Ce code est à utiliser par les rédacteurs pour la condensation des messages.

DIFFUSION RESTREINTE

Ce document ne doit être communiqué qu'aux personnes qualifiées pour le connaître.

ÉDITION D'OCTOBRE 65

Code tactique de condensation, ministère des Armées, octobre 1965, dépliant cartonné imprimé sur 4 volets recto-verso, 10,5 x 13,5 cm.
Il était destiné à être mis dans la poche pour les chiffreurs en manœuvres (coll. Musée des transmissions).

l'armée en temps de guerre. Ses arguments sont repris et affinés en 1883 par Auguste Kerckhoffs[9] dans un ouvrage consacré à la cryptographie militaire. Les études de Lewal et Kerckhoffs permettent d'asseoir des bases théoriques indispensables et des définitions claires. Une prise de conscience existe sur le fait que la mise en place et le respect de procédures garantissent autant la sécurité des transmissions que l'efficacité du système de chiffrement.

Les nombreuses études qui éclosent dans le dernier quart du 19e siècle permettent l'émergence de concepts clairs « qui permettent de distinguer le principe d'un mécanisme cryptographique des variations qui peuvent lui être données au jour le jour, par le choix de paramètres secrets d'un format concis [c'est la clef de chiffrement] »[10]. Les méthodes de cryptographie restent collées à la pratique et sont l'œuvre d'ingénieurs, de linguistes, de militaires, de policiers qui ont une approche pragmatique des procédés de chiffrement et s'inquiètent de leur adaptation à l'usage du télégraphe. Il s'agit donc d'une réponse à un souci d'adaptation technologique. Outre le ministère des Affaires étrangères, tous les grands services de l'État (ministère de la Guerre, de la Marine, de l'Intérieur, des Postes) se dotent de services de chiffres dont l'organisation, le fonctionnement et la déontologie commencent à être fixés.

La cryptologie mécanique

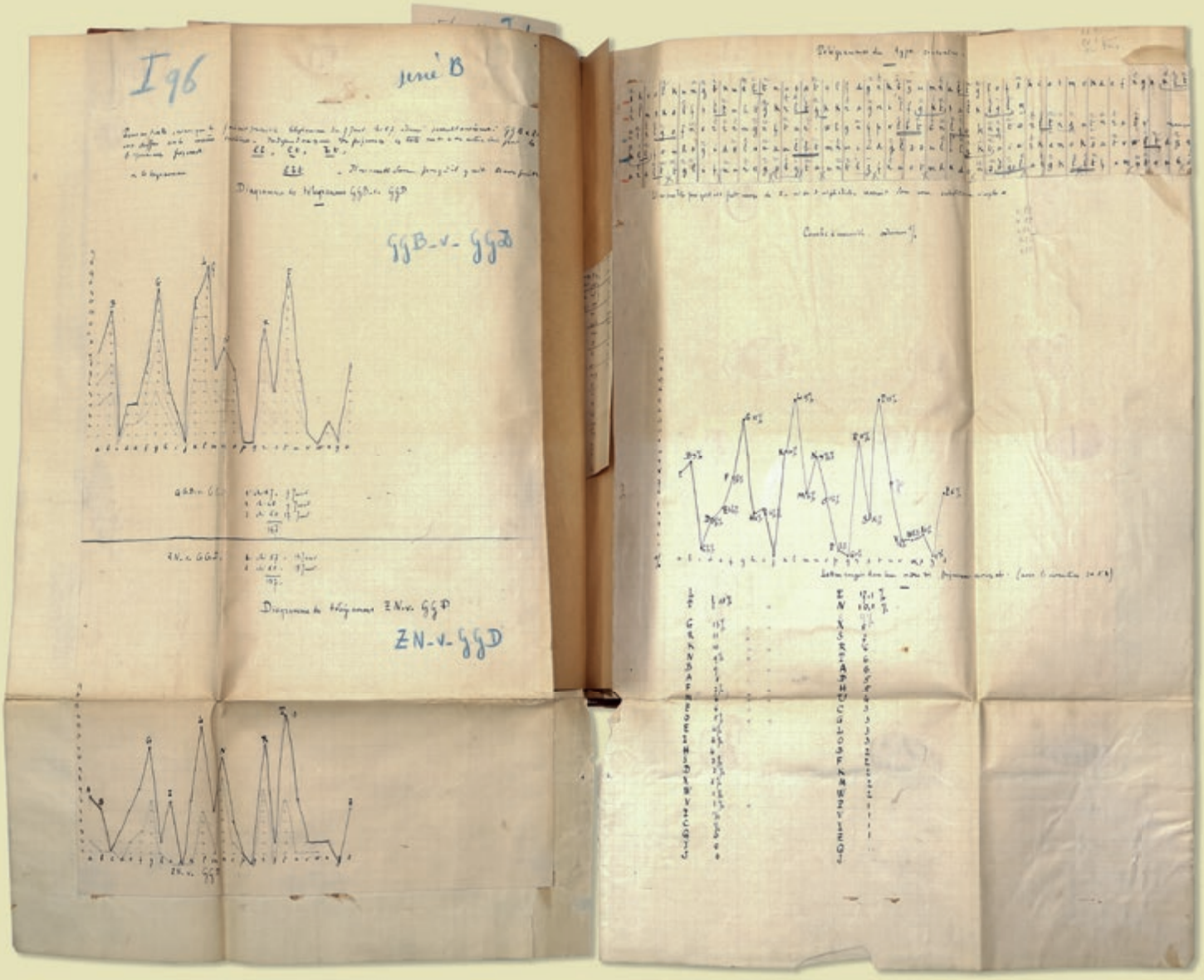
À la fin de la Première Guerre mondiale, il est devenu évident pour les responsables des états-majors que les méthodes « manuelles » de chiffrement et de déchiffrement ont atteint leurs limites. Le volume des communications par la télégraphie explose et laisse les services du chiffre des différents belligérants noyés sous les dépêches à déchiffrer. La complexification des procédés de chiffrement mobilise des équipes des cryptanalystes pendant des jours, parfois des semaines, avant de réussir à casser un chiffre. L'une des préoccupations devient alors la rapidité du chiffrement en mécanisant cette fonction.

Avant même la fin du conflit, des ingénieurs cherchent à mécaniser l'action de chiffrement et déposent des brevets. Ainsi, en 1917, l'américain Edward Hugues Hebern établit les plans d'une machine à roues. Dans le même temps, le Hollandais H. A. Koch dépose en octobre 1918 un brevet pour une machine similaire, suivi par le Suédois Arvid Damm en 1919. Deux de ces brevets seront repris par des industriels quelques années plus tard, et les machines qui en sont issues s'affronteront en équipant chacune l'un des camps opposés. La machine de Koch, produite par une entreprise allemande, deviendra Enigma[11], tandis que le modèle de Damm est racheté par un Suédois, Boris Hagelin, qui fournit les armées françaises et américaines avec ses modèles.

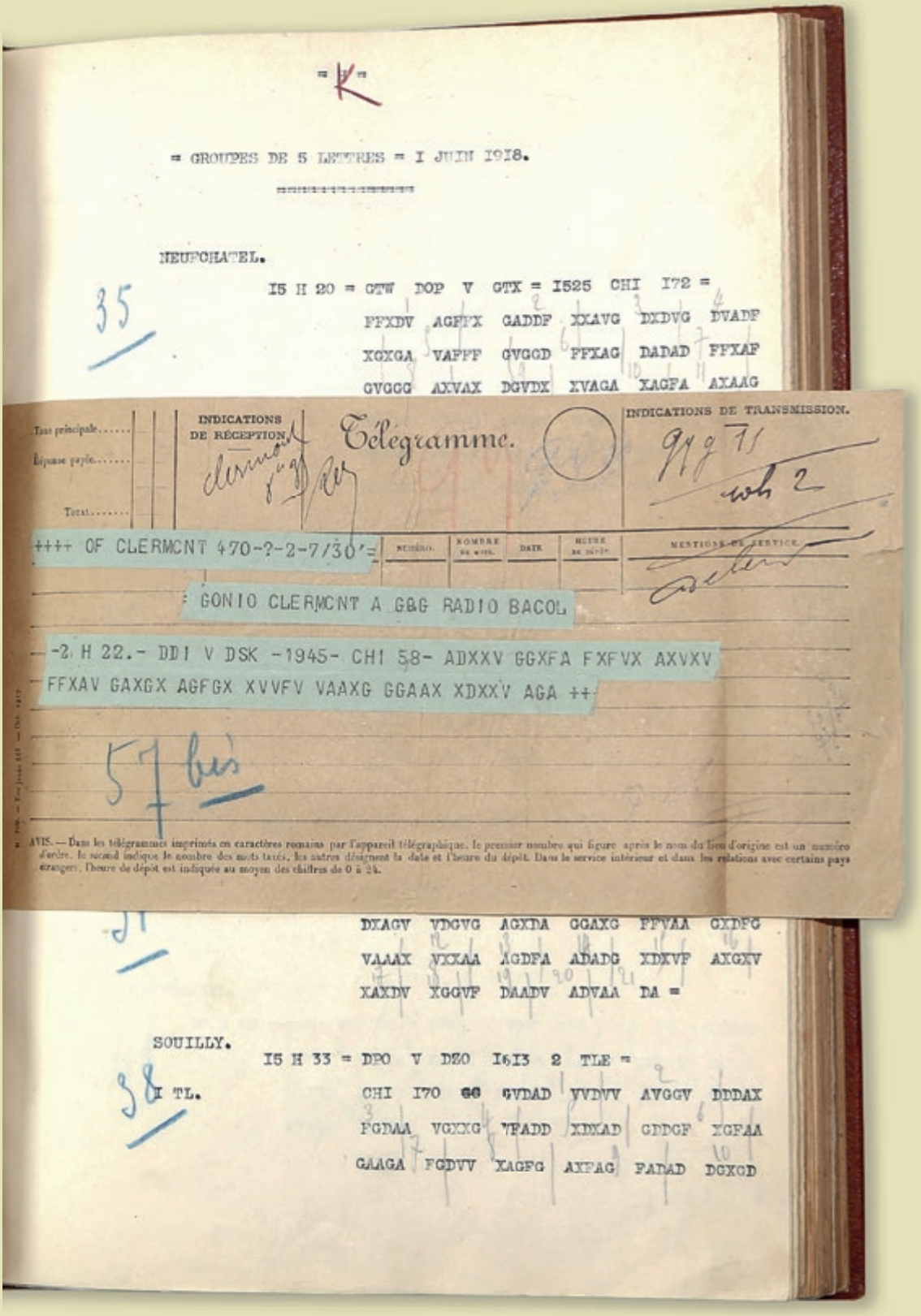
De l'extérieur, ces machines sont assez semblables les unes aux autres. Le plus souvent de l'apparence et de la taille d'une machine à écrire, pesant un peu plus d'une dizaine de kilos, elles possèdent des caractéristiques communes : un clavier servant à taper le texte en clair ou en chiffré ; un système de roues mobiles et interchangeables fixées sur un axe, chacune dotée d'un alphabet dans le désordre. Il n'y a pas de moteur : c'est l'enfoncement des touches du clavier qui entraîne la rotation des roues à alphabet, d'où leur catégorisation en machines mécaniques. Il n'existe pas de système d'impression, tout au moins dans les premiers temps (cette possibilité n'apparaît qu'à la demande du bénéficiaire). Enfin, elles ne sont reliées à aucun système de transmissions.

L'efficacité de ces machines provient des innombrables possibilités de combinaisons de chiffrement offertes par le nombre de roues. C'est d'ailleurs pour cette raison qu'Enigma avait la réputation d'être inviolable : ses différentes modalités de câblage permettaient un nombre de possibilités équivalent à 5 suivi de douze zéros. Il est d'ailleurs intéressant de noter que le développement de ces machines est parallèle à celui des calculateurs. Au cours de la Seconde Guerre mondiale, la machine Colossus mise au point par Alan Turing à Bletchley Park, à la demande des services de renseignements britanniques, n'est autre qu'un calculateur super-puissant destiné à tester les innombrables possibilités de chiffres recueillis par les services d'écoutes de l'armée britannique. Jacques Stern souligne là le lien très fort existant entre la naissance de l'informatique et la cryptologie : « L'apparition des machines à chiffrer permet de se dégager des contraintes physiques et d'enchaîner des opérations multiples. Du coup, le besoin de théorie se fait de nouveau sentir et la parole est de nouveau rendue aux mathématiciens »[12].

Pendant la Première Guerre mondiale, on avait découvert le moyen d'écouter les conversations téléphoniques. Aussi faut-il noter l'effort de recherche et les premiers essais de cryptophonie, pour protéger les conversations entre Churchill et Roosevelt. Mais aucun des moyens développés ne fut satisfaisant avant la numérisation de la parole. Après la Seconde Guerre mondiale, le principal moyen de transmission de messages chiffrés reste la télégraphie.



Graphique d'analyse fréquentielle nécessaire au déchiffrement des codes allemands, travail de Georges Painvin (1886-1980), cryptanalyste à l'État-major de l'armée française pendant la durée de la Première Guerre mondiale, célèbre pour avoir cassé le code allemand ADFGVX en 1918 (coll. Musée Champollion).



= K =

= GROUPES DE 5 LETTRES = I JUIN 1918.

NEUFCHATEL.

35

I5 H 20 = GTW DOP V GTX = I525 CHI I72 =

FFXDV AGFFX GADDF XXAVG DXDVG DVADF

XGXGA VAFFF GVGGD FFXAG DADAD FFXAF

GVGGG AXVAX DGVDX XVAGA XAGFA AXAAG

Taxe principale.....
Réponse payée.....
Total.....

INDICATIONS DE RÉCEPTION

Télégramme.

INDICATIONS DE TRANSMISSION.

9 h 9 71

wh 2

++++ OF CLERMONT 470-?-2-7/30'=

NUMÉRO | NOMBRE DE MOTS | DATE | HEURE DE DÉPÔT | MENTIONS DE SERVICE

GONIO CLERMONT A G&G RADIO BACOL

-2 H 22.- DDI V DSK -1945- CHI 58- ADXXV GGXFA FXFVX AXVXV

FFXAV GAXGX AGFGX XVVFV VAAXG GGAAX XDXXV AGA ++

57 bis

AVIS. — Dans les télégrammes imprimés en caractères romains par l'appareil télégraphique, le premier nombre qui figure après le nom du lieu d'origine est un numéro d'ordre, le second indique le nombre des mots taxés, les autres désignent la date et l'heure du dépôt. Dans le service intérieur et dans les relations avec certains pays étrangers, l'heure de dépôt est indiquée au moyen des chiffres de 0 à 24.

DXAGV VDGVG AGXDA GGAXG FFVAA GXDFG

VAAAX VXXAA AGDFA ADADG XDXVF AXGXV

XAXDV XGGVF DAADV ADVAA DA =

SOUILLY.

I5 H 33 = DPO V DZO I6I3 2 TLE =

38 I TL.

CHI I70 GG GVDAD VVDVV AVGGV DDDAX

FGDAA VGXXG VFADD XDXAD GDDGF XGFAA

GAAGA FGDVV XAGFG AXFAG FADAD DGXGD

Exemple de télégramme chiffré allemand, intercepté
par un poste français, 1er juin 1918 (coll. Musée Champollion).

Au lendemain de cette guerre et pendant la guerre froide, le chiffre demeure un outil réservé à l'usage exclusif des États. De chaque côté du rideau de fer, les pays avancés en ce domaine engagent des moyens considérables pour le développement de puissantes mesures de cryptanalyse. Ces moyens sont d'ailleurs considérés comme du matériel de guerre. Les gouvernements de tous les pays ont gardé un silence presque total sur les moyens cryptologiques.

La révolution technologique de 1976 : la cryptologie moderne

À partir des années 1970, le développement de la cryptologie sort du domaine militaire et diplomatique pour tomber dans le domaine civil ou commercial. Cette évolution reste difficile à tracer du fait de la confidentialité des archives. L'une des principales raison en est le développement des échanges informatiques de nature financière et commerciale. Les milieux d'affaires en ressentent le besoin et exercent des pressions pour imposer la mise en place des moyens de protection de leur flux d'informations.

Le NBS (National Bureau of Standards) lance un appel à candidature pour un procédé susceptible d'être utilisé largement pour de telles transactions. IBM remporte la compétition en 1977 avec le « Data Encryption Standard », qui est un algorithme reposant sur un procédé classique, la clé de chiffrement symétrique. Utilisé pour l'authentification de données, il devient l'algorithme le plus utilisé dans le monde : on le trouve dans les puces des cartes bancaires ou de la carte Vitale, les cartes SIM (Subscriber Identification Module) des téléphones cellulaires ou encore dans les décodeurs de télévision à péage comme celui de Canal +. En 1990, un nouvel algorithme de chiffrement symétrique est publié par Xuejia Lai et James Massey et exploité par la société Mediacrypt. C'est l'un des meilleurs systèmes à ce jour, qui n'a officiellement pas encore été décrypté.

La cryptologie est aujourd'hui un pilier d'un vaste ensemble, celui de la sécurité de systèmes d'informations. La nature des informations protégées a changé : il ne s'agit plus de protéger des informations confidentielles ou secrètes, mais de contribuer au bon fonctionnement d'installations ou d'infrastructures sensibles telles que des calculateurs utilisés dans les centrales d'énergie, les réseaux de communication ou de distribution, ou encore les circuits financiers, et que l'on dénomme également des infrastructures vitales[13].

À travers cette évolution retracée à grands traits, on perçoit deux tendances. La première est une démocratisation et une banalisation progressives. D'abord réservée au cercle étroit des plus hautes autorités de l'État dans les seuls domaines de la diplomatie ou des affaires militaires, la nécessité de protéger les informations s'étend désormais à tous les domaines de l'activité humaine, depuis le chef de l'État jusqu'au simple consommateur dans ses transactions quotidiennes. On peut donc considérer que la protection de l'information est une condition incontournable, inhérente à la société dans laquelle nous vivons, où l'information est devenue une ressource comme une autre, parce qu'elle permet d'établir un ingrédient indispensable à tout échange : la confiance.

Valérie Caniart

ORIENTATIONS BIBLIOGRAPHIQUES :

— Arboit, Gérald, *L'émergence d'une cryptographie militaire en France*, note historique n° 15, juillet 2008 (www.cf2r.org)

— Caniart, Valérie, « Écritures cachées, écritures codées : guerre et stratégie », in *Cacher Coder, 4000 ans d'écritures secrètes*, Figeac, Musée Champollion-Les écritures du monde, 2015

— Ceillier, Rémi, *La cryptographie*, Paris, PUF, coll. « Que sais-je ? », 1948

— Eyraud, Charles, *Précis de cryptographie moderne*, 2e édition, 1959

— Fletcher Pratt, Murray, *Histoire de la cryptographie. Les écritures secrètes depuis l'Antiquité jusqu'à nos jours*, Paris, Payot, 1940

— Kerckhoffs, Auguste, *La cryptographie militaire, ou Des chiffres usités en temps de guerre*, Paris, Librairie militaire L. Baudoin, 1883

— Lerville, Edmond, *Les cahiers secrets de la cryptographie. Le chiffre dans l'histoire, des histoires du chiffre*, Monaco, Éditions du Rocher, 1972

— Lewal, Jules-Louis, *Études de guerre. Tactique du renseignement*, 2 vol., Paris, Librairie militaire L. Baudoin, 1881. Réédition en 2013

— Ministère de l'Intérieur (service du chiffre), *Manuel d'instruction*, n° 142

— Ministère de la Guerre, *Notions élémentaires de cryptographie*, exemplaire n° 115, Paris, Imprimerie nationale, 1920

— Ollier, Alexandre, *La cryptographie militaire avant la guerre de 1914*, Panazol, Lavauzelle, 2002

— Secrétariat général du gouvernement, *Étude cryptographique*, n° 1/50, 1955

— Secrétariat général du gouvernement, *Terminologie interministérielle de cryptographie à l'usage des spécialistes du chiffre*, n° 1499, Paris, 1956

— Stern, Jacques, *La science du secret*, Paris, Odile Jacob, 1998

— Valerio, Paul, *De la cryptographie : essai sur les méthodes de déchiffrement*, Paris, Librairie militaire L. Baudoin, 1893

— Wrixon, Fred B., *Langages secrets. Codes, chiffres et autres cryptosystèmes*, Cologne, Könemann, 2000

Notes

1 — In *La science du secret*, 1998 (voir bibliographie)

2 — Ce texte, retrouvé en 1987 dans les Archives ottomanes d'Istanbul, décrit l'analyse fréquentielle des lettres d'un texte chiffré et explique que le nombre et la répartition des caractères (lettres ou symboles) dans un texte offre des pistes pour le décoder. Voir aussi, sur al-Kindi, l'article d'Hervé Lehning p. 46.

3 — Edmond Lerville, *Les cahiers secrets*, p. 31-32 (voir bibliographie)

4 — Voir à ce sujet l'article d'Hervé Lehning, p. 46.

5 — Charles Eyraud, *Précis de cryptographie moderne*, p. 9 (voir bibliographie)

6 — Murray Fletcher Pratt, *Histoire de la cryptographie…*, p. 1198-99 (voir bibliographie)

7 — Gérald Arboit, *L'émergence d'une cryptographie militaire en France* (voir bibliographie)

8 — Jules Lewal, *Études de guerre. Tactique du renseignement…* (voir bibliographie)

9 — Auguste Kerckhoffs, *La cryptographie militaire…* (voir bibliographie)

10 — Jacques Stern, *La science du secret* (voir bibliographie)

11 — Sur la machine Enigma, voir l'article de Christian Westerhoff et Thomas Weis p. 62.

12 — Jacques Stern, op. cit., p. 11

13 — Jacques Aubert (sous la dir. de), *Cryptologie : la science du secret*, Cesson-Sévigné, AAMTAT, 2012, p. 2